MACLEANS.CA

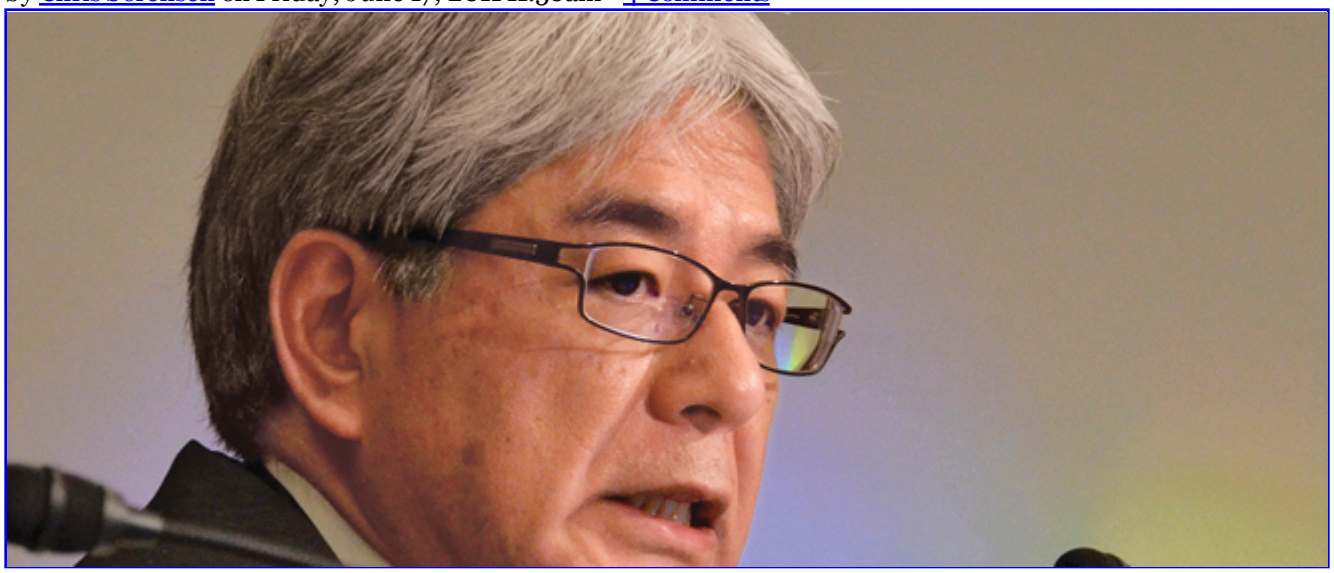
Gold Winner MAGAZINE OF THE YEAR (DIGITAL)

Categories: Science & Technology, Technology

Hacker attack

A rash of high-profile thefts reveals just how unsafe the Internet we depend on has become

by Chris Sorensen on Friday, June 17, 2011 11:50am - 4 Comments



Yoshikazu Tsuno/AFP/Getty Images

Visitors to the Conservative Party of Canada's website last Tuesday were confronted with a shocking message: the Prime Minister had been rushed to hospital in Toronto after choking on a hash brown. Media outlets scrambled to unearth more details about the breakfast-hour emergency only to learn that it was all a big joke. The party's website had been hacked.

It didn't take long to find out who was behind the prank. A group calling itself LulzRaft claimed responsibility on Twitter, and later followed up by breaking into the party's donor database and posting names and emails of more than 5,000 people online. Why did they do it? "The Conservative party was really just a hack of opportunity," wrote someone purporting to be the hacker in an anonymous email to *Maclean's*. "We noticed the vulnerability and realized we could easily create some lulz, and draw some media attention without hurting anyone." For the

uninitiated, “lulz” is Web-slang for laughs—derived from the abbreviation LOL, for “laugh out loud.”

But the Tories aren’t laughing. Nor should they be. It’s an embarrassing breach of security for a governing party that, just a few months earlier, assured Canadians that it had a cyber-security strategy in place. It’s also the latest in a string of brazen attacks on high-profile targets around the globe, ranging from Sony Corp. and Google Inc. to defence contractor Lockheed Martin and the International Monetary Fund. In addition to attention-seekers like LulzRaft, experts say many more hackers are quietly working on behalf of organized crime and even foreign governments—so much so that Washington is now talking about cyberattacks as a potential “act of war.”

“We have guys in their basements doing horrible things to these humongous companies and governments,” says Brad Haines, an Edmonton-based hacker and security consultant who goes by the online handle RenderMan. So just imagine, he says, what a dedicated criminal organization or well-funded foreign government could accomplish.

The sobering reality is that, as more of our lives and livelihoods are moved online, the more tantalizing the targets become for cybercrooks. At the same time, security experts say many of our defences are still stuck in the 1990s, if they exist at all. For those with short memories, that was a time when viruses like Melissa and Michelangelo merely threatened to clog our networks, not steal from us. And if we can’t even stop the glory-seeking “hacktivists,” who announce their every move, how are we supposed to protect ourselves from those with more sinister intentions? “There’s an old joke about how we are losing the war on drugs,” says Haines, who figures the Harper hack was made possible by something as mundane as out-of-date software or a weak password. “It means that we are losing the war to people *on drugs*. I mean, how bad can we get?”

To get a sense of what kind of damage a few angry computer geeks can do, consider the cyberflogging that Sony—a computer and electronics company, no less—has endured over the past few months. The firm’s troubles appear to have originated from a series of skirmishes with customers who wanted to modify their PS3 game consoles to run a Linux operating system. It ultimately resulted in Sony taking one hacker to court.

It didn’t take long before hackers operating under the name Anonymous decided to retaliate. The loose-knit group has also taken responsibility for attacks against the Church of Scientology, the controversial Westboro Baptist church and, most notably, PayPal, Visa and Mastercard in response to those firms’ decision to stop enabling financial contributions to WikiLeaks. With apparently little effort, hackers managed to steal personal data from 77 million Sony PlayStation Network customers, forcing Sony to temporarily shut down the popular online game-playing network in April.

It didn’t end there. A hacker group calling itself LulzSec taunted Sony in a May 31 post on Twitter: “Hey @Sony, you know we’re making off with a bunch of your internal stuff right now and you haven’t even noticed? Slow and steady, guys.” LulzSec, whose Twitter page is called “The Lulz Boat” (which explains the name of the smaller, copycat LulzRaft group that targeted Harper), also released what it claimed was source code for the Sony Computer Entertainment Development Network on June 6. Later that week, Sony acknowledged an attack on its Sony Pictures website, and that 37,500 visitors to the site had passwords, emails, and other potentially identifying details stolen.

The people behind LulzSec have also claimed responsibility for several other prominent hacks in recent months. They include: broadcaster PBS, whose website was hacked to post a story claiming that dead rapper Tupac Shakur was still alive; an Atlanta-based FBI contractor called InfraGard, which resulted in data about its user base being posted on the Web; and Nintendo, although LulzSec stressed via Twitter it wasn’t upset with the Japanese game-maker: “We like the N64 too much—we sincerely hope Nintendo plugs the gap.”

Suffice it to say, Sony’s new-found status as the Internet’s favourite whipping boy has been a public relations nightmare, costing it an estimated US$173 million. Its stock is down about 10 per cent since the beginning of the month. And while the Japanese company is working with law enforcement to capture the culprits—three hackers

were arrested in Spain just last week—most security experts say that apprehending a couple of computer nerds is unlikely to solve the problem (Anonymous is believed to have hundreds of members all over the world). "Yes, it's criminal and it's wrong, but there are much larger issues out there," says Haines. "We have to give our information to these companies and they're not protecting it properly."

As it turns out, however, even the companies whose raison d'être is network security are struggling. Earlier this year, a firm called RSA, a subsidiary of EMC Corp., was the victim of what it referred to as an "extremely sophisticated cyberattack" that compromised some 40 million of the company's SecurID tokens. The tokens generate authentication codes every 30 or so seconds and are given to employees of client companies so they can log in to secure networks with an extra level of security. It's believed that the compromised tokens were later used in an attack against Lockheed Martin, although the defence contractor said in May that it stopped the attack before any data was stolen.

Such well-planned, multi-stage attacks suggest these hackers are interested in more than just bragging rights. It raises the possibility of a systematic campaign on behalf of a government or some other politically motivated group. "Why would you breach Lockheed Martin? Because you're after a country's defence technology secrets," says Anup Ghosh, the founder and CEO of browser security company Invincea and a former program manager at the U.S. Defense Advanced Research Projects Agency, or DARPA.

Google, too, has found itself in the crosshairs of a sophisticated hacker campaign, apparently emanating from China. The search giant says passwords and emails from hundreds of Gmail accounts were stolen by Chinese hackers in a bid to target senior U.S. government officials, activists and others.

It's not only the private sector that's at risk. Late last week the IMF acknowledged a breach of its systems, while earlier this year the CBC reported that two Canadian government departments and one agency—Finance, the Treasury Board and Defence Research and Development Canada—were targeted. Ottawa eventually confirmed an "unauthorized attempt" to access the Treasury Board's network, but said there were "no indications that any data relating to Canadians was compromised." The U.S. government has also been a target, and said recently that cyberattacks could be considered an "act of war," forcing a conventional response. "If you shut down our power grid, maybe we will put a missile down one of your smokestacks," an unnamed military official was recently quoted as saying in the *Wall Street Journal*. On the other hand, the U.S. and Israel are believed to be behind a worm called Stuxnet that targeted Iran's nuclear capabilities.

Equally likely, however, is that hackers are seeking government information that can be used for financial gain. Briefing notes about trade policy. Emails discussing a pending corporate merger. Drug approvals. The possibilities are endless. "It's a wholesale theft of a nation going on right now," says Ghosh, adding that many breaches likely go unreported—particularly among U.S. government agencies where there is little upside to going public. "These networks are getting compromised: federal, civilian, DOD [U.S. Department of Defense]. They are in our networks stealing terabytes of data every day. On a national level, it's the loss of economic competitiveness with other countries." Ghosh claims that, although none will admit it, most government departments buy the exact same off-the-shelf security systems that everyone else uses—much of which he says were originally developed in the 1990s. "The threat has radically evolved since then, but our defences have not," he says. "It's time for us to realize we are fighting the current war with the tools of the last war." This could be one reason why instances of hacking appear to be on the rise, with some experts predicting a banner year for data breaches in 2011.

It's not only state secrets that can yield big returns for cybercrooks. A 2010 report by the University of Toronto's Munk School of Global Affairs explored one St. Petersburg gang that earned about $2 million a year with a simple but effective scheme called Koobface (an anagram for Facebook). It involved setting up fake social networking accounts and then sending links to unwitting "friends," promising a video of the recipient captured naked by a hidden webcam. "One click leads down a Kafka-esque rabbit hole of viruses and Trojan horses," according to the report. How did the gang make money? The compromised computers engaged in thousands of micro-transactions in multiple countries around the globe, often for less than a penny each. The transactions included things like

clicking on online ads or downloading fake anti-virus software packages, with each hit generating a small cut for the gang.

A similar approach could also yield big returns in stock or currency trading schemes, according to Rafal Rohozinski, a principal at the Ottawa-based security firm the SecDev Group, which was involved in the Koobface report. Hackers could also team up with white-collar crooks looking to make money off of stock price movements—selling shares short after a major data breach has been revealed and the stock price plummets, only to buy them again before the shares recover. "It's a perfect example of how cybercrime is much bigger and more commonplace than a pimply-faced teenager in the basement eating pizza," says Rohozinski.

While hackers leave digital tracks, the sheer volume of attacks means that most operate with near-impunity because law enforcement agencies simply don't have the resources to go after them. The Munk study, for example, said that Bell Canada records in the order of 80,000 new attacks per day on computers on its network. Nor does it help that most hackers, like those behind Koobface, tend to operate in foreign countries where local law enforcement has other priorities, creating an environment where computer crimes are viewed as a relatively risk-free endeavour. "If you look at the people involved in hacking, the centre of gravity is not in places like North America, it's in places like Russia or, increasingly, places like Nigeria," Rohozinski says. "For them, stealing or bilking a bank account owner in Toronto of his earnings is a hell of a lot safer than engaging in a knife fight over a fistful of rubles in a back alley in Russia."

In 1994, the *New York Times* described the Internet as "a new Wild West" when it came to security. It's still very much that way. Only now it's littered with steamer trunks containing our most important valuables—many of them with their locks rusted or missing.

Tags: Anonymous, Google, hackers, Lockheed Martin, LulzSec, Sony, Stephen Harper

Recommend Send 3 recommendations. Sign Up to see what your friends recommend.

0

Print

SHARE

More by Chris Sorensen

- **How Kia and Hyundai became cool**

  Once the butt of jokes, the South Korean companies are suddenly the fastest-growing automakers

- **Turning the pages**

  Marc Tellier is racing to rescue the Yellow Pages by dragging it into the digital age

- **Novak Djokovic: the man to beat**

  Does Djokovic's rise to the top of the ranking spell the end of the Nadal-Federer era?

4 Comments

PreviousA Wii problem

NextCanada Post is all but obsolete

From Macleans

- **Beyond The Commons**

Jack Layton's letter to Canadians

"I want to share with you my belief in your power to change this country and this world"

- **Canada**

Inside the fight of Jack Layton's life

His confidants and caucus colleagues recount the difficult days before and after his shocking announcement

- **Canada**

The life and times of Jack Layton

The NDP leader has left a lasting legacy on Canadian politics

- **Video**

Video: Jack Layton's post-election speech

Relive Layton's rousing address following the NDP's unprecedented election results

- **Jesse Brown**

The RCMP and Montreal police ignored cybercrime while demanding new powers to fight cybercrime

The "David Mabus" case raises serious questions about law enforcement's interest in catching online criminals

- **Health**

A radical new rabies treatment

For the first time people are surviving the infection without vaccinations—but is this therapy too risky?

- **Business**

Top 50 socially responsible corporations

These companies are making corporate social responsibility a key part of the business plan